

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

**THIS PAGE BLANK (USPTO)**



Europäisches Patentamt  
European Patent Office  
Office européen des brevets

⑪ Veröffentlichungsnummer:

**0 008 086**  
**A1**

⑫

## EUROPÄISCHE PATENTANMELDUNG

⑬ Anmeldenummer: 79102784.0

⑮ Int. Cl.<sup>3</sup>: **H 04 K 1/06**

⑭ Anmeldetag: 02.08.79

⑯ Priorität: 04.08.78 DE 2834281

⑰ Anmelder: **SIEMENS AKTIENGESELLSCHAFT Berlin und München, Postfach 261, D-8000 München 22 (DE)**

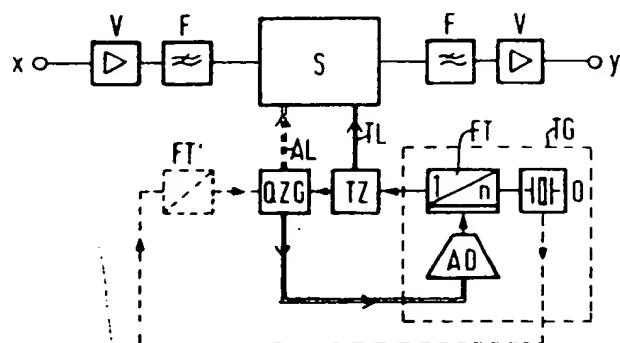
⑲ Veröffentlichungstag der Anmeldung: 20.02.80  
Patentblatt 80/4

⑳ Erfinder: **Brusch, Josef, Fasanenstrasse 22, D-8025 Unterhaching (DE)**

㉑ Benannte Vertragsstaaten: **BE CH DE FR GB IT LU NL**

### ㉒ Anordnung zur Durchführung einer verschleierten Übertragung von Informationen.

㉓ Die Erfindung betrifft eine Anordnung zur Durchführung einer verschleierten Übertragung von Informationen, insbesondere Sprache, mittels einer steuerbaren Speichereinrichtung (S), in die auf der Sendeseite die anfallenden Informationen in Zeitelemente (1, 2, 3, 4, 5; 1', 2', 3', 4', 5') unterteilt hintereinander eingespeichert und zueinander zeitvertauscht für ihre Übertragung wiederum ausgespeichert sind und in der auf der Empfangsseite diese Vertauschung der Zeitelemente rückgängig gemacht ist, und bei der die Steuertakte für die Speichereinrichtung auf der Sende- und der Empfangsseite jeweils vom Takt des Taktgenerators (TG) abgeleitet sind. Hierbei wird zum Verwischen der Zeitgrenzen der Zeitelemente mit dem Ziel eines erhöhten Sicherheitsgrades der Taktgenerator in seiner Frequenz steuerbar ausgeführt und seine Frequenzsteuerung pseudozufällig mittels eines Quasizufallsgenerators (QZG) vorgenommen.



**EP 0 008 086 A1**

SIEMENS AKTIENGESELLSCHAFT  
Berlin und München

Unser Zeichen

78 P 6706

Anordnung zur Durchführung einer verschleierten Über-  
tragung von Informationen

Die Erfindung bezieht sich auf eine Anordnung zur Durch-  
führung einer verschleierten Übertragung von Informa-  
tionen, insbesondere Sprache, mittels einer steuerbaren  
10 Speichereinrichtung, in die auf der Sendeseite die an-  
fallenden Informationen in Zeitelemente unterteilt hin-  
tereinander eingespeichert und zueinander zeitverzögert  
für ihre Übertragung wiederum ausgespeichert sind und  
in der auf der Empfangsseite diese Vertauschung der Zeit-  
15 elemente wieder rückgängig gemacht ist und bei der die  
Steuertakte für die Speichereinrichtung auf der Sende-  
und der Empfangsseite jeweils vom Takt eines Taktgene-  
rators abgeleitet sind.

20 Anordnungen dieser Art dienen insbesondere bei Sprech-  
funknetzen dazu, das Mithören von Gesprächen durch Un-  
befugte zu unterbinden. Wie beispielsweise die Litera-  
turstelle "Brown Boveri Mitteilung 6-74", Seiten 266  
bis 269 angibt, kann für die Sprachverschleierung von

zwei grundsätzlichen Möglichkeiten Gebrauch gemacht werden, nämlich der Frequenzvertauschung und der Zeitelementvertauschung. Im Hinblick auf den technischen Aufwand ist der Zeitelementvertauschung der Vorzug zu geben.

5 Die Zeitelementvertauschung hat jedoch den Nachteil, daß sie sich von Unbefugten leichter entschleiern läßt und zwar über das sogenannte "Segmentieren" des verschleierten Signals, d.h. das Auffinden der Grenzen der einzelnen aufeinanderfolgenden Zeitelemente.

10

Der Erfindung liegt die Aufgabe zugrunde, für eine Anordnung zur Durchführung einer verschleierten Übertragung von Informationen mittels Zeitelementvertauschung eine weitere Lösung anzugeben, die dieses Segmentieren des verschleierten Signales durch Unbefugte wesentlich erschwert.

Ausgehend von einer Anordnung zur Durchführung einer verschleierten Übertragung von Informationen, insbesondere Sprache, mittels einer steuerbaren Speichereinrichtung, in die auf der Sendeseite die anfallenden Informationen in Zeitelemente unterteilt, hintereinander eingespeichert und zueinander zeitvertauscht für ihre Übertragung wiederum ausgespeichert sind und in der auf der Empfangsseite diese Verteilung der Zeitelemente wieder rückgängig gemacht ist und bei der die Steuertakte für die Speichereinrichtung auf der Sendeseite und der Empfangsseite jeweils vom Takt eines Taktgenerators abgeleitet sind, wird diese Aufgabe gemäß der Erfindung dadurch gelöst, daß der Taktgenerator in seiner Frequenz steuerbar ist und daß seine Frequenzsteuerung pseudozufällig mittels eines Quasizufallsgenerators vorgenommen ist.

35 Der Erfindung liegt die wesentliche Kenntnis zugrunde, daß sich die Zeitgrenzen der aufeinanderfolgenden, in

ihrer Zeitlage miteinander vertauschten Zeitelemente in außerordentlich einfacher Weise ohne Eingriff in den eigentlichen Steuerteil variieren lässt, wenn die Taktfrequenz der gemeinsamen Taktversorgung pseudozufällig 5 in geringen Grenzen geändert wird. Zwar bleibt hierbei der Informationsinhalt eines Zeitelementes erhalten, d.h. die Information wird lediglich über die Zeitachse pseudozufällig verlängert oder verkürzt. Dies ist jedoch für die Erschwernis des Segmentierens eines verschleierten Signals ausreichend, weil ja der Informationsinhalt eines Zeitelementes selbst nicht vorhersehbar ist.

Zweckmäßig weist der Quasizufallsgenerator eine sehr 15 große Pulswiederholungsperiode auf, wodurch das Erkennen der Periodizität der Zeitvariation ebenfalls erschwert wird. Gegebenenfalls kann es in diesem Zusammenhang sinnvoll sein, den Quasizufallsgenerator programmierbar auszuführen.

20

Um die durch die Variation der Zeitgrenzen der Zeitelemente verursachten Störungen der übertragenen Informationen vernachlässigbar klein zu halten, ist es sinnvoll, die Frequenzvariation der Steuertakte in den 25 Grenzen von ca.  $\pm 10\%$  festzulegen.

Bei einer bevorzugten Ausführungsform ist der Steuertakt für den Quasizufallsgenerator ebenfalls vom Takt des Taktgenerators abgeleitet.

30

Anhand zweier in der Zeichnung dargestellten Ausführungsbeispiele soll die Erfindung noch näher erläutert werden. In der Zeichnung bedeuten Fig. 1 das Blockschaltbild einer Anordnung zur Durchführung einer verschleierten Übertragung nach 35 der Erfindung,

Fig. 2 ein erstes Zeitelement-Vertauschungsschema  
Fig. 3 eine Speichereinrichtung zur Durchführung einer  
Zeitelementvertauschung nach Fig. 2  
Fig. 4 ein zweites Zeitelement-Vertauschungsschema  
5 Fig. 5 eine Speichereinrichtung zur Durchführung einer  
Zeitelementvertauschung nach Fig. 4.

Das Blockschaltbild nach Fig. 1 zeigt eine Anordnung  
zur Durchführung der Verschleierung von zu übertragen-  
10 den Informationen, wie sie auf der Sendeseite für die  
Verschleierung und auf der Empfangsseite für die Ent-  
schleierung zu verwenden ist. Die an der Anschlußklem-  
me x ankommenden Informationen werden zunächst im Ver-  
stärker V verstärkt und nach ihrer Begrenzung im Fil-  
15 ter F der eigentlichen Speichereinrichtung S zugeführt.  
Die Speichereinrichtung S wird über die Taktleitungen  
T1 mit den nötigen Steuertakten der Taktzentrale TZ  
versorgt, die wiederum diese Steuertakte vom Takt des  
Taktgenerators TG ableitet. Auf der Ausgangsseite der  
20 Speichereinrichtung S folgt zunächst wieder ein Filter  
F zur Frequenzbandbegrenzung, dessen Ausgangssignal  
über den Verstärker V der Anschlußklemme y zugeführt  
ist.

25 Wie Fig. 1 zeigt, ist der Taktgenerator TG in seiner  
Frequenz pseudozufällig über den Quasizufallsgenerator  
QZG gesteuert, der seinen Takt ebenfalls von der Takt-  
zentrale TZ erhält. Der Taktgenerator TG besteht hier-  
zu aus einem festen Frequenzoszillator O hoher Fre-  
30 quenzkonstanz, beispielsweise ein Quarzoszillator,  
dessen Taktfrequenz wesentlich höher gewählt ist als  
die Frequenzen der Steuertakte. Dem Festfrequenzoszil-  
lator O ist der steuerbare Frequenzteiler FT nachge-  
schaltet, dessen Teilungsverhältnis n:1 über den Quasi-  
35 zufallsgenerator QZG pseudozufällig verändert wird.  
Hierzu ist ein Adressendecoder AD vorgesehen, der die

vom Quasizufallsgenerator gelieferten Codeadressen in ein analoges Steuersignal umwandelt.

Wie die Darstellung in unterbrochener Linie zeigt, kann 5 der Quasizufallsgenerator QZG seinen Takt anstelle von der Taktzentrale TZ unmittelbar vom Festfrequenzoszillator O über einen festen Frequenzteiler FT' erhalten. Von dieser Variante kann Gebrauch gemacht werden, wenn es nicht gewünscht wird, daß der Quasizufallsgenerator 10 die Frequenzvariation des Taktgenerators TG mitmacht.

Bei Ausbildung der Speichereinrichtung S nach Fig. 3 für eine Zeitvertauschung der Zeitelemente nach Fig. 2 liefert der Quasizufallsgenerator QZG nach Fig. 1 über 15 die Adressenleitungen A1 fortlaufend Codeadressen an die Speichereinrichtung, mit deren Hilfe die in der Speichereinrichtung S vorzunehmende Zeitelementverwaltung pseudozufällig durchgeführt wird.

20 Wie das Zeitelement-Vertauschungsschema nach Fig. 2 zeigt, werden in der Speichereinrichtung S bei einer Ausbildung nach Fig. 3 jeweils fünf aufeinanderfolgende Zeitelemente 1,2,3,4,5 bzw. 1',2',3',4',5' von der Zeitdauer  $t_0$  miteinander vertauscht, wobei die Vertauschung 25 entsprechend den vom Quasizufallsgenerator QZG nach Fig. 1 gelieferten Codeadressen variiert wird. Die zeitrichtige Einspeicherung und die zeitvertauschte Aus- speicherung der Zeitelemente erfolgt bei der Speicher- einrichtung nach Fig. 3 digital. Hierzu weist sie ein- 30 gangsseitig einen Umsetzer A/D auf, der ausgangsseitig die digitalisierten Informationen über den Umschalter A wechselweise dem Schieberegister SR1 und SR2 zuführt. Während der Einspeicherung von fünf Zeitelementen in das Schieberegister SR1 wird das Schieberegister SR2 35 ausgelesen und umgekehrt. Die Auslesung erfolgt für das Schieberegister SR1 über den Multiplexer M1 und

für das Schieberegister SR2 über den Multiplexer M2. Beide Multiplexer variieren die Auslesung der Zeitelemente im Sinne der gewünschten Vertauschung in Abhängigkeit der vom Quasizufallsgenerator über die Adressenleitung Al gelieferten Codeadressen, die im Adressenumwerter AU in für die Multiplexer geeignete Steuersignale umgesetzt werden. Auf der Ausgangsseite der Multiplexer ist wiederum ein Umschalter U2 vorgesehen, der wechselweise im Rhythmus der Einspeicherung der 10 eingangsseitig anfallenden Informationen in die Schieberegister SR1 und SR2, die über die Multiplexer M1 und M2 ausgespeicherten vertauschten Zeitelementfolgen dem Umsetzer D/A zuführt, auf dessen Ausgangsseite die 15 ursprünglich analogen Informationen wiederum in analoger, jedoch verschleierter Form abgegeben werden.

Bei einer Ausführung der Speichereinrichtung S nach Fig. 5 wird die Zeitvertauschung von fünf Zeitelementen 1,2,3,4,5 bzw. 1',2',3',4',5' die jeweils einen Informationsabschnitt ZA bilden, entsprechend Fig. 4 in der Speichereinrichtung durch Inversion dieser Informationsabschnitte herbeigeführt. Als Speicher finden bei der Speichereinrichtung nach Fig. 5 zwei sogenannte "RAM"-Speicher Verwendung, die in Verbindung mit einer geeigneten Steuerung die gewünschte Inversion automatisch liefern. Im folgenden wird dieser Speichertyp als "filo"-Speicher (first in - last out - Speicher) bezeichnet. Die von links ankommenen Signale werden zunächst wie bei der Speichereinrichtung nach Fig. 3 im Umsetzer 30 A/D in digitale Signale umgewandelt und anschließend über den eingangsseitigen Umschalter U1 wechselweise einem der beiden "filo"-Speicher zugeführt. Ein- und Ausgang haben bei diesen Speichern einen gemeinsamen Anschluß. Jeweils im Zeittakt einer Ausspeicherung 35 werden die eingespeicherten Informationsabschnitte in invertierter Form über den Umschalter U2 dem Umsetzer

D/A zugeführt, der die Digitalsignale wieder in Analogsignale umwandelt und diese ausgangsseitig in der gewünschten verschleierten Form zur Verfügung stellt.

- 5 Die Entschleierung der übertragenen Signale auf der Empfangsseite erfolgt in der Speichereinrichtung S auf die gleiche Weise wie auf der Sendeseite, lediglich in umgekehrter Richtung.
- 10 Die Synchronisation von Sende- und Empfangszeit kann in üblicher Weise durch zusätzliche Übertragung von Synchronisiersignalen aufrechterhalten werden. In gleicher Weise kann die Anfangssynchronisation für den Taktgenerator und den Quasizufallsgenerator durch eine
- 15 Vorabinformation für die Ausgangsstellung des empfangsseitigen Quasizufallsgenerators erfolgen.

Es versteht sich von selbst, daß die Umsetzer A/D und D/A in der Speichereinrichtung S entfallen können, wenn 20 die zu verschleiernden Informationen digitale Signale sind.

5 Patentansprüche

5 Figuren

Patentansprüche

1. Anordnung zur Durchführung einer verschleierten Übertragung von Informationen, insbesondere Sprache, mittels einer steuerbaren Speichereinrichtung, in die auf der Sendeseite die anfallenden Informationen in Zeitelemente unterteilt hintereinander eingespeichert und zueinander zeitvertauscht für ihre Übertragung wiederum ausgespeichert sind und in der auf der Empfangsseite diese Vertauschung der Zeitelemente wieder rückgängig gemacht ist und bei der die Steuertakte für die Speichereinrichtung auf der Sende- und der Empfangsseite jeweils vom Takt eines Taktgenerators abgeleitet sind, dadurch gekennzeichnet, daß der Taktgenerator (TG) in seiner Frequenz steuerbar ist und daß seine Frequenzsteuerung pseudozufällig mittels eines Quasizufallsgenerators (QZG) vorgenommen ist.
2. Anordnung nach Anspruch 1, dadurch gekennzeichnet, daß der Quasizufallsgenerator (QZG) eine sehr große Pulswiederholungsperiode hat.
3. Anordnung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der Quasizufallsgenerator (QZG) programmierbar ausgeführt ist.
4. Anordnung nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die pseudozufällig gesteuerte Frequenzvariation des Taktgenerators (TG) für eine Variation der Steuertakte in den Grenzen von ca.  $\pm 10\%$  festgelegt ist.

0008086

78 P 6706

- 2 -

5. Anordnung nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß der Steuertakt für den Quasizufallsgenerator (QZG) ebenfalls vom Takt des Taktgenerators (TG) abgeleitet ist.

0008086

1/2

FIG1

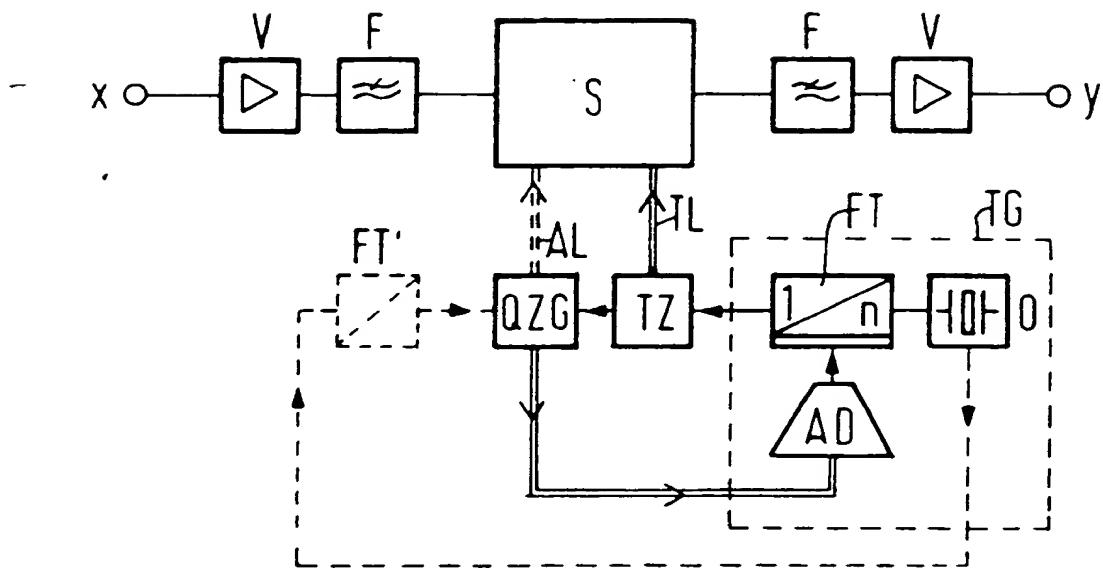


FIG 2

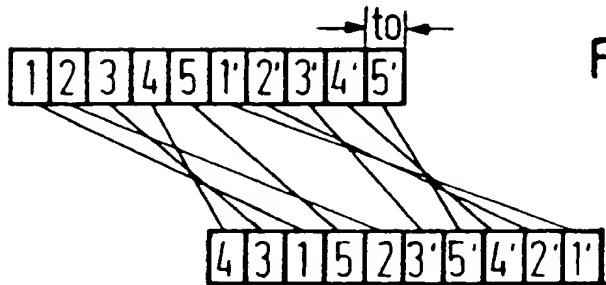


FIG 4

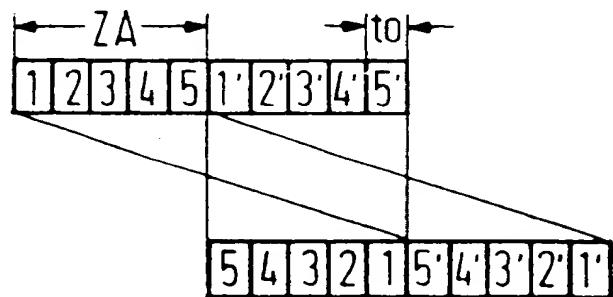


FIG3

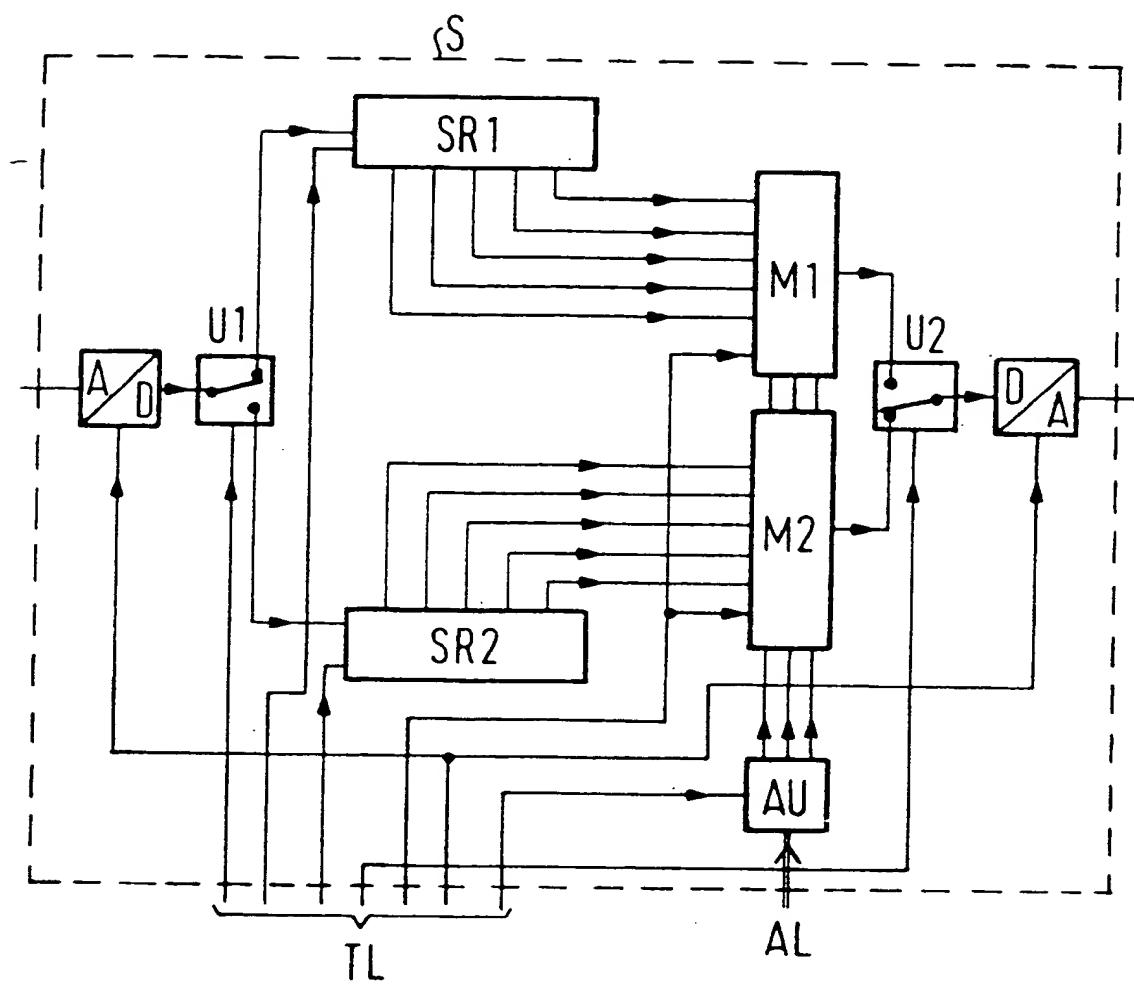
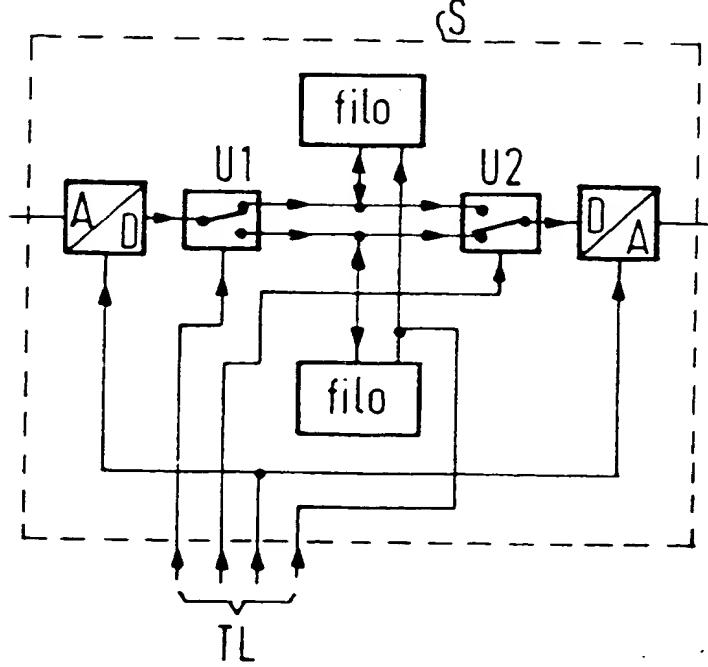


FIG5





| EINSCHLÄGIGE DOKUMENTE  |   |                   | KLASSIFIKATION DER ANMELDUNG (Int.CI. 1)   |
|---|---|-------------------|--|
| Kategorie   | Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile   | betrifft Anspruch |  |
|   | <p><u>DE - A - 2 412 732 (LICENTIA)</u><br/>           * Seite 4, zweiter Abschnitt;<br/>           Seite 12, Zeilen 6-15; Seite 14, letzter Abschnitt *</p> <p>---</p> | 1                 | H 04 K 1/06  |
| A   | <p><u>DE - C - 2 307 441 (LICENTIA)</u><br/>           * Spalte 2, Zeile 54 - Spalte 3,<br/>           Zeile 9; Spalte 4, Zeilen 19-43 *</p> <p>-----</p>               | 1                 | RECHERCHIERTE<br>SACHGEBIETE (Int. Cl. 1)<br><br>H 04 K 1/06<br>1/00   |
|   |   |                   | KATEGORIE DER<br>GENANNTEN DOKUMENTE<br><br>X: von besonderer Bedeutung<br>A: technologischer Hintergrund<br>O: nichtschriftliche Offenbarung<br>P: Zwischenliteratur<br>T: der Erfindung zugrunde liegende Theorien oder Grundsätze<br>E: kollidierende Anmeldung<br>D: in der Anmeldung angeführtes Dokument<br>L: aus andern Gründen angeführtes Dokument<br>&: Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument |
| <p>b   Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt.</p> |   |                   |  |
| Recherchenort   | Abschlußdatum der Recherche   | Prufer            |  |
| Den Haag  | 06.11.1979  | HOLPER            |  |

**THIS PAGE BLANK (USPTO)**